GUIDA COMPARATIVA

Confronto tra Akamai Guardicore Segmentation e le soluzioni di microsegmentazione tradizionali

Impareggiabile visibilità

Per comprendere cosa succede nel vostro ambiente, è essenziale disporre della visibilità necessaria sulle comunicazioni tra i carichi di lavoro. Una visibilità davvero efficace consente di sapere, in ogni momento, cosa avviene per ogni carico di lavoro insieme a tutto il relativo contesto. Inoltre, le funzionalità di raggruppamento e filtraggio per le risorse e le regole sono essenziali per creare le policy appropriate in modo semplice e veloce.

Akamai	Microsegmentazione tradizionale
Facile visualizzazione dell'intero ambiente L'agente di Akamai Guardicore Segmentation è un firewall basato su host che viene eseguito su sistemi operativi moderni e preesistenti, fornendo piena visibilità sui flussi di rete a livello di processi e servizi per i sistemi operativi Windows e Linux, insieme alla copertura degli endpoint MacOS.	**Visibilità parziale dei sistemi preesistenti** Nessuna visione dei sistemi operativi Microsoft Windows precedenti a Windows 2002. Ciò è dovuto al fatto che l'agente delle soluzioni di microsegmentazione tradizionali si basa su un firewall Windows, disponibile solo nei sistemi successivi alla versione 2002. Per i sistemi Linux, questo agente supporta solo la visibilità L4.
Contesto completo e impareggiabile Per quanto riguarda la visibilità, disporre del contesto e dei dettagli più appropriati risulta di fondamentale importanza. La nostra soluzione raccoglie, oltre ai dati dei flussi, anche il relativo contesto critico, come le informazioni sui processi, i file, il livello di patch e molto altro.	**Contesto minimo** Vengono raccolte solo le informazioni su flussi e computer, il che fa perdere importanti dettagli sul contesto, come processi e file. Pertanto, il processo di comprensione delle dipendenze delle applicazioni risulta più laborioso e dispendioso in termini di tempo.
Nessuna limitazione al tipo o al numero di etichette Non abbiamo impostato alcuna limitazione al numero o al tipo di etichette utilizzabili per offrire la flessibilità necessaria e il supporto derivante dalla conoscenza di ulteriori casi di utilizzo. Ciò elimina la necessità di tradurre le etichette dai database di gestione delle configurazioni (CMDB) e altre origini dati.	**Etichettatura rigida** Con una gerarchia di etichettatura fissa e predefinita, le soluzioni tradizionali obbligano a etichettare le applicazioni solo con un numero prestabilito, indipendentemente dai singoli requisiti dell'ambiente e dalle specifiche esigenze aziendali.
Etichettatura basata sull'IA Il rilevamento e l'etichettatura di applicazioni basate sull'IA aiutano a identificarle se manca un CMDB affidabile e ad assegnare loro automaticamente l'etichetta corretta.	**Non si dispone di un CMDB? È un problema difficile da risolvere...** Con l'etichettatura manuale e una gerarchia di etichette preconfigurata, se l'organizzazione non dispone di un CMDB, il processo di etichettatura diventa estremamente complicato.

Akamai

Copertura leader del settore

Uno degli elementi chiave di una buona soluzione di microsegmentazione è la possibilità di proteggere le risorse più importanti a prescindere dalla posizione in cui vengono distribuite o a cui vi si accede: un sistema legacy o moderno, Windows o Linux, on-premise o virtualizzato, all'interno di container e molto altro.

Akamai	Microsegmentazione tradizionale
Supporto completo per Windows e Linux Gli agenti di Guardicore sono supportati su tutti i sistemi operativi Windows e Linux (sia nuovi che legacy), poiché la nostra soluzione è indipendente dall'infrastruttura sottostante.	**Supporto Windows e Linux limitato** L'applicazione delle policy dipende dal firewall Windows, per gli ambienti Windows, e dagli iptables, per gli ambienti Linux, il che implica, inevitabilmente, una protezione limitata o nessuna protezione per alcuni sistemi operativi Windows legacy e nessuna regola a livello di processo L7 per gli ambienti Linux.
Supporto completo dei container Visibilità completa per gli ambienti containerizzati e utilizzo dei controlli CNI (Container Network Interface) per l'applicazione delle policy.	**Supporto limitato dei container** L'applicazione delle policy si basa su iptables e calcoli di policy back-and-forth, che non sono scalabili in un ambiente di container e causano problemi di latenza e downtime.

Creazione di policy semplici in modo rapido

Un buon motore di policy consente di esprimere il proprio intento con il più piccolo numero di regole possibile, senza applicare restrizioni al linguaggio delle policy. Inoltre, aiuta a ridurre al minimo il lavoro di gestione delle policy offrendo procedure guidate e operazioni automatizzate.

Akamai	Microsegmentazione tradizionale
Consenso e negazione Sono supportate regole di elenchi di elementi consentiti/bloccati e metodi intermedi per consentire ai team addetti alla sicurezza di rispondere rapidamente a ogni scenario, eliminando la necessità di inserire negli elenchi di elementi consentiti ogni singolo flusso legittimo.	**Inserimento negli elenchi di elementi consentiti con supporto limitato delle regole di negazione** L'aderenza a un modello di creazione di elenchi di elementi consentiti, che risulta sicuro, ma dispendioso in termini di tempo, non consente alle tradizionali soluzioni di microsegmentazione di rispondere automaticamente alle minacce note che devono essere bloccate rapidamente.
Modelli di policy per una varietà di casi di utilizzo Modelli pronti all'uso e workflow di creazione delle policy per scenari comuni: mitigazione ransomware, isolamento delle applicazioni, segmentazione dell'ambiente e molto altro. I modelli consentono di risparmiare tempo e di ridurre gli errori umani.	**Set di modelli limitato** I modelli di segmentazione sono supportati principalmente in ambienti Microsoft. Non sono supportati modelli per i comuni casi di utilizzo della segmentazione, come le misure di isolamento, mitigazione e correzione del ransomware.
Criteri di policy completi I criteri di policy possono includere origine, destinazione, porte, protocolli, processi, servizi (ad es. l'utilità di pianificazione comunemente usata dai ransomware), utenti e nomi di dominio completi (FQDN).	**Criteri limitati** Nessuna policy a livello di processo L7 per i sistemi operativi Linux e nessuna possibilità di creare policy basate sui singoli servizi di Microsoft Windows.

La sicurezza prima di tutto

Per contrastare le minacce alla sicurezza complesse, come i ransomware, è necessario un approccio completo alla sicurezza. Anche se la segmentazione viene prescritta dal National Institute of Standards and Technology (NIST) e dalla Casa Bianca come una risposta fondamentale, è necessario un approccio integrato alla sicurezza e al rilevamento delle violazioni per tenere al sicuro l'organizzazione.

Akamai	Microsegmentazione tradizionale
Prevenzione e mitigazione dei ransomware Akamai Guardicore Segmentation offre modelli pronti all'uso per tutte le fasi della kill chain degli attacchi, dalla prevenzione al contenimento fino alla mitigazione.	**Nessun modello ransomware** Le soluzioni tradizionali hanno capacità limitate di bloccare gli attacchi ransomware con modelli pronti all'uso.
Interrogazione degli endpoint per il rilevamento delle minacce e la conformità Insight, il nostro strumento basato su osquery, consente di interrogare server ed endpoint in tempo reale per la conformità e il rilevamento dei malware.	**Nessun rilevamento in tempo reale** Le soluzioni tradizionali non possono rilevare in tempo reale le attività dannose nel data center.
Funzionalità di rilevamento Basato su una tecnologia brevettata, l'agente di Akamai Guardicore Segmentation reindirizza le sessioni bloccate e non riuscite su un motore di rilevamento dinamico per consentire di eseguire ulteriori operazioni di analisi e messa in quarantena.	**Nessuna possibilità di messa in quarantena** Le soluzioni tradizionali sono prive delle funzionalità di individuazione e della capacità di rilevare o mettere in quarantena i computer con indicatori di compromissione (IoC) noti.
Team gestito per la ricerca delle minacce Akamai offre servizi gestiti per la ricerca delle minacce che estendono le capacità del team di sicurezza in sede e consentono all'organizzazione di tenersi al passo con le minacce più recenti.	**Nessun servizio di ricerca delle minacce** I fornitori tradizionali non sono in grado di offrire servizi di ricerca delle minacce basati sulla loro soluzione, che possono risultare un fattore distintivo molto importante rispetto all'escalation di ransomware e malware.
Firewall di intelligence sulle minacce Per prevenire i comportamenti dannosi noti, Akamai Guardicore Segmentation blocca gli IP, i file e gli hash dannosi tramite regole di firewall automatiche.	**Nessun feed sulle minacce** Poiché non dispongono di una simile funzionalità, le soluzioni tradizionali non possono arrestare l'accesso a e da noti IP e URL dannosi.

Operazioni o performance e latenza

Una bassa latenza è di importanza critica per un progetto di segmentazione di successo. Ciò significa che è necessario essere in grado di scalare la policy con più regole, etichette per risorse e altri oggetti di policy, il tutto senza introdurre una latenza aggiuntiva.

Akamai

Motore ottimizzato per la latenza

Il nostro motore di segmentazione è stato creato per scenari su larga scala grazie ad un meccanismo di filtraggio ottimizzato che offre un tempo di latenza praticamente non suscettibile alle dimensioni delle policy.

Microsegmentazione tradizionale

Più regole portano a una maggiore latenza

Gli agenti introducono più latenza man mano che crescono il numero e le dimensioni delle regole. Gli iptables di Linux non erano stati creati per scalare il traffico est-ovest delle imprese. Ne risulta una latenza significativa che cresce direttamente insieme alle dimensioni delle policy.

Per ulteriori informazioni su Akamai Guardicore Segmentation o per richiedere una demo del prodotto personalizzata, visitate il sito akamai.com/it/guardicore.

 | Supporto | | Data di pubblicazione: 07/23